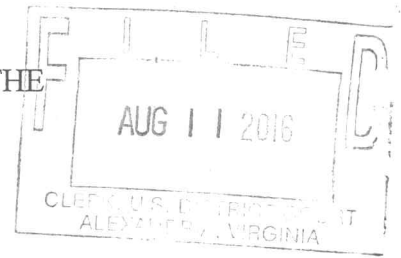


# EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA  
Alexandria Division



IN RE SEARCH WARRANTS  
INVOLVING NICHOLAS YOUNG

)  
)  
)

No. 1:16 sw 455

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Nicholas Caslen, after being duly sworn, depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), assigned to the Washington Field Office, Joint Terrorism Task Force ("JTTF"). I have been an FBI Special Agent since 2011, and worked on the JTTF in both Wichita, Kansas, and Washington, D.C. As part of my duties, I investigate potential criminal and terrorism-related activities associated with suspected Homegrown Violent Extremists. I have participated in numerous counterterrorism investigations, during the course of which I have conducted physical surveillance, executed court authorized search warrants, and used other investigative techniques to secure relevant information regarding various crimes.

2. This affidavit is submitted in support of warrants to search the following locations or things:

- a. The contents of a backpack seized from Nicholas Young upon his arrest on August 3, 2016, including a black Casio Verizon G'z One flip-phone; and a black Amazon tablet model SV98LN;
- b. One black 2003 Dodge Dakota pickup truck, bearing Vehicle Identification Number 1D7HG38N23S289168, and Virginia license tags WITNSME; and
- c. One black AT&T ZTE GoPhone, found on a truck transporting Nicholas Young's 2003 Dodge Dakota pickup truck on August 3, 2016; and

- d. Locker #45 at Franconia/Springfield Metropolitan Transit Police Department's District 2 substation.

Based on the facts set forth in this affidavit, there is in these locations or things, evidence more particularly described on Attachment A, of attempts to provide material support to a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B.

3. I am familiar with facts contained in the affidavit sworn to in this Court on August 2, 2016, by my colleague, FBI Special Agent David Martinez, in support of a criminal complaint to arrest Nicholas Young. I adopt the facts contained in the Special Agent Martinez's affidavit ("the Criminal Complaint Affidavit") as true statements for this affidavit and incorporate them here.

4. In addition to the facts contained in the Criminal Complaint Affidavit, the information contained in this affidavit is based on my personal knowledge and observations made during the course of this investigation, personal review of records, documents, and other physical evidence obtained during this investigation, including recorded telephone, audio, and in-person communications and information provided to me by FBI Agents and other government personnel with knowledge relating to this investigation.

5. Since this affidavit is submitted for the limited purpose of establishing probable cause, I have not included every fact known to me concerning this investigation. When I assert that a statement was made by an individual, that statement is described in substance and in part, but my assertion is not intended to constitute a verbatim recitation of the entire statement.

6. In addition to the information contained in the Criminal Complaint Affidavit, I can add that, on August 3, 2016, the FBI arrested Young at Washington Metro Area Transit Authority Headquarters located at 600 5th St NW, Washington D.C., on the basis of the criminal

complaint and arrest warrant issued by this Court the previous day. Young was searched incident to arrest and, in his pocket was found a folded white piece of paper with the name of the mobile messaging account provider and the account name for “Young’s First MM Account” (as referenced in Paragraph 49 of the Criminal Complaint Affidavit).

A. The Contents of a Backpack

7. At the time of his arrest, Young also had on his person a backpack. The backpack was searched incident to arrest. In the backpack, the arresting agents found a July 23, 2016 receipt from an electronics store in Fairfax, Virginia, for the purchase of ten gift cards (the gift cards were marketed through the same internet service provider that was described in Paragraph 50 of the Criminal Complaint Affidavit). A FBI agent went to that electronics store identified in the receipt, and obtained from that store another copy of that same transaction receipt. The electronics store also provided a copy of video surveillance from the store. The surveillance video appears to reflect Young in the store and purchasing the gift cards at the time reflected on the receipt.

8. Also in the backpack at the time of Young’s arrest were an open but empty package for an AT&T ZTE GoPhone; a black Casio Verizon G’z One flip-phone; and a black Amazon tablet model SV98LN. Neither the Casio Verizon G’z One flip-phone nor the Amazon tablet bore an observable serial number on its outside case.

9. After Young’s arrest, Young requested that the agents power-off the cell phone, but the agents declined his request. Based on my knowledge and experience, I know that once cell phones are turned off, many require a pass code in order to be operated again. Based on Young’s sophistication with electronic devices (as described in the Criminal Complaint Affidavit), I

suspect that Young's request to power off his cell phone was motivated by his desire that the phone be turned off so that the FBI would not subsequently be able to unlock it.

10. Based on my knowledge and experience, I know that tablets such as the one located in Young's backpack are capable of running the mobile messaging application that Young used to communicate with UCO2 as described in the Criminal Complaint Affidavit. Moreover, as explained in the Criminal Complaint Affidavit, there is probable cause to search electronic and communication devices possessed and/or used by Nicholas Young.

B. One Black 2003 Dodge Dakota Pickup Truck

11. According to the records of the Virginia Department of Motor Vehicles, as of July 31, 2016, Nicholas Young, of 12737 Heron Ridge Drive, Fairfax, Virginia, was the registered owner of a 2003 black Dodge Dakota pickup truck, bearing Vehicle Identification Number 1D7HG38N23S289168, and Virginia license tags WITNSME.

12. On August 3, 2016, Young drove his 2003 Dodge Dakota to his place of employment with WMATA at the Franconia/Springfield Metro Station. After Young's arrest, a Metro Police K-9 officer and dog did a sweep of the exterior of the vehicle. The dog gave a positive alert for hazardous material. The vehicle was subsequently prepared for transport atop a flatbed truck to a secure location. Prior to transport, an inventory was taken of the contents of the interior of the vehicle. In the inventory, investigators found one Kel-Tec .380 firearm, an empty magazine, six hollow point rounds, and \$1,065 in cash.

C. One black AT&T ZTE GoPhone

13. Young's Dodge Dakota pickup truck was transported atop a flatbed truck to a secure location in Washington, D.C. FBI agents followed the transport vehicle and never lost sight of it



during the trip. Once the vehicle arrived at the secure location, the driver of the flatbed truck noticed and told FBI agents about a cell phone that was lying on the bed of the flatbed truck. Agents then found a black cell phone on the bed of the flatbed truck below (and between) the rear wheels of Young's Dodge Dakota. Agents collected the cell phone and identified it as a black ZTE cell phone with clear tape over its camera aperture. As noted above, agents searching Young's backpack upon his arrest found an open but empty package for an AT&T ZTE GoPhone.

14. As noted in the Criminal Complaint Affidavit, Young used "burner" phones for security purposes. Based on my knowledge and experience, an AT&T GoPhone is a prepaid phone that is readily used as a "burner" phone. Further, that phone can operate the mobile messaging account that Young utilized to communicate with UCO2.

15. Metro Police reviewed their security camera footage and provided a copy of the footage showing that on the day of the arrest, Young went to his vehicle and appeared to be handling something underneath his truck. I believe that the phone found on the tow truck was a phone used by Young and hidden underneath his Dodge Dakota, but dislodged in the course of the transport to Washington, D.C., from the Franconia Springfield Metro station.

D. Locker #45 at MTPD District 2 Substation

16. According to the Metro Transit Police Department, Young was assigned a locker at the Franconia/Springfield MTPD District 2 substation. On August 3, 2016, a Metro Transit Police officer showed FBI agents Young's locker, identified as locker number 45 on the second floor, inside the MTPD men's locker room. The locker is approximately six feet in height, two feet in width, and two feet in depth, and was secured by a combination lock. That same day,

Metro Transit Police opened the combination lock, and FBI agents replaced it with a different lock to safeguard the contents of the locker pending acquisition of a warrant to search that locker.

17. When he was arrested at work, Young had on his person a receipt for the purchase of ten gift cards. As noted in the Criminal Complaint, however, Young sent 16 gift card codes. No receipt for the remaining gift cards was found in the course of the search of Young's residence that was conducted shortly after his arrest. As a result (and unless they have been destroyed or discarded), records of his purchase of the remaining six gift cards are likely to be in his locker or in his truck.

18. Based on my knowledge, training and experience, as well as that of other agents assigned to this investigation from the FBI, I know that receipts and related records are often found in people's vehicles, as well as in their workplaces. In this case, these records include records relating to income, assets, and expenditures, and are likely to be relevant to Young's purchase of gift cards for transmission to CHS and ISIL in July 2016, as well as assets that he sought to send overseas in 2015. Such records are also likely to be relevant to his contacts with terrorist groups in the past, and his past travel or attempts to travel overseas to fight on behalf of terrorist groups.

19. Based on my knowledge, training and experience, as well as that of other agents assigned to this investigation from the FBI, I know that these important records are often maintained in hard copy and/or digital form, such as on computers and other electronic devices. This application seeks permission to search and seize records that might be found in Young's tablet, phones, or other electronic devices. One form in which records might be found is stored

on the hard drive or other storage media of a computer or other electronic devices. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

20. I know that Young uses electronic devices and is sophisticated about computer matters. As described in the Criminal Complaint Affidavit, Young not only showed a pro-ISIL video to CHS on YouTube and later explained to CHS how to set up an email account that would be difficult to trace back to CHS, but also - - in his attempts to communicate with CHS - - actually communicated with UCO2 through a text message, through that email account, and later through a mobile messaging application. Young told UCO that Young used “burner” phones (as described in Paragraph 16 of the Criminal Complaint Affidavit), and appeared to use one such “burner” phone in order to transmit the codes from the gift cards to UCO2 last month; after all, he used two different accounts of the mobile messaging application in order to communicate with CHS’s Mobile Messaging Account. In addition, as explained in Paragraph 21 of the Criminal Complaint Affidavit, Young told UCO that Young believed that the U.S. government was spying on Young through Young’s electronic devices.

21. Moreover, as described in the Criminal Complaint Affidavit, Young spoke to FBI agents in September 2010; on that occasion, he told the FBI that he maintained a Facebook page. As described in the Criminal Complaint Affidavit, he also spoke to law enforcement authorities on June 1, 2015; on that occasion, he told the interviewing officers that he used an internet dating site. Further, in June 2012, a fellow officer in the Metro Transit Police who was then close



friends with Young told the FBI that Young regularly used the internet and blogged on websites that he visited.

22. Based on the information described above, there is probable cause to believe evidence will be found in Young's tablet, phones, and electronic media for at least the following reasons:

a. Based on my knowledge and training, I know that computer files or remnants of computer files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the storage medium that is not currently being used by an active file - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media- in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or

application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

23. In light of these concerns, I request authority to seize the tablet, phones, electronic media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to search the hardware for the evidence described. I further seek authority to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers and other electronic media were used, the purpose of their use, who used them, and when.

#### Conclusion

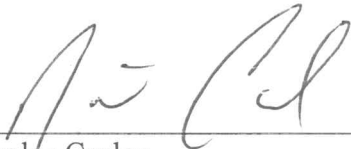
24. The backpack, phone, and truck that I now seek to search are all now in the custody of the FBI in Washington, D.C. Pursuant to the USA PATRIOT ACT, enacted in October 2001, Rule 41 of the Federal Rules of Criminal Procedure now authorizes warrants to be issued by a Federal magistrate judge in any district in which activities related to terrorism may have occurred, for property outside the district.

25. Based upon the above facts (as well as those included in the Criminal Complaint Affidavit), there is probable cause to believe that Nicholas Young attempted to provide material support to a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B, and that evidence of this crime, more particularly described on Attachment A, is likely to be found in the following locations and things:

- a. The contents of a backpack seized from Nicholas Young upon his arrest on August 3, 2016, including a black Casio Verizon G'z One flip-phone; and a black Amazon tablet model SV98LN;
- b. One black 2003 Dodge Dakota pickup truck, bearing Vehicle Identification Number 1D7HG38N23S289168, and Virginia license tags WITNSME; and
- c. One black AT&T ZTE GoPhone, found on a truck transporting Nicholas Young's 2003 Dodge Dakota pickup truck on August 3, 2016; and
- d. Locker #45 at Franconia/Springfield Metropolitan Transit Police Department's District 2 substation.

Wherefore, I request the issuance of search warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

FURTHER THIS AFFIANT SAYETH NOT.

  
\_\_\_\_\_  
Nicholas Caslen  
Special Agent, FBI

Subscribed to and sworn before me on this 11th day of August 2016.

\_\_\_\_\_/s/   
\_\_\_\_\_  
John F. Anderson  
United States Magistrate Judge  
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A - ITEMS TO BE SEIZED

1. All records and documents, however maintained, that concern the international transfer of money or assets, or the procurement of any item that may have been involved in or in support of terrorist or violent acts, including photographs, correspondence, and safe deposit keys.
2. All records and documents, however maintained, referring or relating to identities or aliases of Nicholas Young.
3. All records and documents, however maintained, referring or relating to past travel or planned travel by Nicholas Young, including airline tickets, credit card bills, bank records, checks, itineraries, passports, and visas.
4. Any and all records, documents, invoices and materials that concern any accounts with any internet service provider;
5. All records, documents, and paraphernalia, however maintained, relating to ISIL/ISIS (or any of its aliases), other designated terrorist groups, or any individual or group engaged in terrorism or terrorist activity, or communications with or involving such groups and/or individuals.
6. All contact lists, however maintained (including but not limited to names, addresses, phone numbers, Internet accounts or usernames, photographs or other identifying information) of individuals associated with Nicholas Young and/or foreign terrorist groups.
7. All records and documents, however maintained, referring or relating to the purchase or use of gift cards, encryption programs, or applications that may be used for clandestine or covert communications.
8. All records and documents, however maintained, referring or relating to any storage facilities, safety deposit boxes, mailboxes, or other locations where any of the foregoing items may be located.
9. Any and all firearms, ammunition, body armor, military-style equipment, or explosive materials or their precursors.
10. Any communications or electronic device capable of storing any of the items to be seized, including but not limited to all cellular phones, smart phones, electronic data processing and storage devices, computers and computer systems, keyboards and other associated peripherals, Central Processing Units, external and/or internal drives, portable drives, external and internal storage devices such as magnetic tapes and/or disks or diskettes, together with system documentation, operating logs, software and manuals, passwords, test keys, encryption codes or similar codes that are necessary to access computer programs, and the stored contents of the items described in this paragraph, which may be searched for only the items listed above.